UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/867,935	05/30/2001	Bjorn Markus Jakobsson	44-6	7747

7590 09/16/2004

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
ZAND, KAMBIZ	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/867,935	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08/03/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09/27/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-19** have been examined.

Drawings

2. The drawings filed on 08/03/2001 have been accepted by Examiner.

Information Disclosure Statement PTO-1449

3. The Information Disclosure Statement submitted by applicant and received on 09/27/2001 has been considered. Please see attached PTO-1449.

Specification

4. The abstract of the disclosure is objected to because the phrase "may" line 5 create ambiguity with respect to claim language and figure 3 where the task transformation is the result of error-related, blinding and permutation operation with no other option presented. Examiner suggests deletion of the phrase "may". Appropriate Correction or clarification is requested.

5. The disclosure is objected to because of the following informalities: the phrase "may", page 2, line 23 create ambiguity with respect to claim language and figure 3 where the task transformation is the result of error-related, blinding and permutation operation with no other option presented. Examiner suggests the following

format: insertion of the phrase "include an error-related operation that" after the phrase "the transformation" and before the phrase "may include replication" **or** deletion of the phrase "may". Appropriate Correction or clarification is requested.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

7. **Claims 1-19** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claims 1, 18 and 19, the relationship between the following steps makes the claims indefinite and unclear in that neither method, means and one or more programs for performing a computational task nor interrelationship of method, means and one or more programs for performing a computational task are set forth in these claims in order to achieve the desired results expressed in "**receiving one or more results of the transformed computational task in the originator machine; and transforming the one or more results of the transformed computational task in the originator machine in a manner which permits verification that the one or more results are appropriate results for the given input**" with respect to claim 1; "**to receive one or more results of the transformed computational task, and to transform the one or more results of the transformed computational task in a manner which permits**

verification that the one or more results are appropriate results for the given input" with respect to claim 18; and **"receiving one or more results of the transformed computational task in the originator machine; and transforming the one or more results of the transformed computational task in the originator machine in a manner which permits verification that the one or more results are appropriate results for the given input"** with respect to claim 19 phrases.

Reasons are as follows:

It is not clear the result received by originator machine is **the result created by the computation within the originator machine and that result is being considered as the received result by the originator machine where it is verified**? (A); **Is the result of the execution of the original result** sent by the originator machine to the other machine that is being transmitted back to the originator machine is the received result where it is verified? (B); and **Is it the same result of the transform computation that is sent** to the other machine by the originator machine that is being transmitted back to the originator machine (not result of the execution of the result)? (c)

Considering any of the above result will lead to different verification procedures once the verification procedure within the originator machine is enabled. As an example: **with respect to A** only the inverse of the computation that leads to the original input and the matching of the two is sufficient for verification; , however in B, the inverse of the ***execution*** result and comparison with the computational result of the function created in

the originator machine may be one way of the verification process; and in C probably the matching of the computational result sent and the same result transmitted back is one way of verification process. **Therefore there is either a missing method steps or means or programming steps or the lack of clarity make the claims unclear and indefinite where such clarity must be present in the claims language.**

Examiner will considers the above unclear phrases in broadest possible interpretation with respect to verification procedure and the result received by the originator machine.

8. **Claims 2-17** are rejected based on their dependency on the rejected independent claim 1 above.

Allowable Subject Matter

9. **Claims 1-19** would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action. Examiner however reserve the right to withdraw the allowances of the claims if the amended claims that overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action, changes the scope of the claim where further search and consideration becomes necessary.

10. The following is an examiner's statement of reasons for allowance:

Chaum (4,759,063) disclose a blind signature system where the output of a blinding operation being inputted to signing transformation and where the permutation operation is being done on a transmitted input of one party to another.

Kocher et al (6,278,783 B1) teach DES and other cryptographic processes with leak minimization for smartcards and other cryptosystems where two keys and two messages performing permutation and blinding operation by Xoring the inputs.

Kocher et al (2001/0002486A1) patent application publication disclose leak-resistant cryptographic method and apparatus using the Chinese Remainder Theorem using blind signature or permutation.

Chaum, Kocher singly or in combination **do not disclose the specific steps** of Applicant's invention where transforming a computational task involving a given input in the originator machine, the transforming of the computational task involving at least an error-related operation, a blinding operation and a permutation operation; sending the transformed computational task to at least one additional machine for execution; and where one or more results are appropriate results for the given input (upon verification procedure) **as recited in the independent claims 1-19.**

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (4,759,063) teach single blind signature system.

b. U.S.Patent No. US (6,327,661 B1) teach using unpredictable information to minimize leakage from cryptosystems.

c. U.S.Patent No. US (6,061,449 A) teach secure processor with external memory using block chaining and block re-ordering.

d. U.S.Patent No. US (6,389,136 B1) teach auto-recoverable and auto-certifiable cryptosystems with RSA or factoring based keys.

e. U.S.Patent No. US (5,878,140 A) teach limited traceability systems.

f. U.S.Patent No. US (6,772,339 B1) teach mix and match: a new approach to secure multiparty computation.

g. U.S.Patent No. US (6,049,613 A) teach method and apparatus for encrypting,decrypting, and providing privacy for data values.

h. EP 1 043 862 A2 disclose generation of repeatable cryptographic key based on varying parameters.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

09/14/04